Mod-p reducibility, the torsion subgroup, and the Shafarevich-Tate group

Amod Agashe *

May 26, 2009

Abstract

Let E be an optimal elliptic curve over $\mathbf{Q}$ of prime conductor N. We show that if for an odd prime p, the mod p representation associated to E is reducible (in particular, if p divides the order of the torsion subgroup of $E(\mathbf{Q})$), then the p-primary component of the Shafarevich-Tate group of E is trivial. We also state a related result for more general abelian subvarieties of $J_0(N)$ and mention what to expect if N is not prime.

1 Introduction and results

Let N be a positive integer. Let $X_0(N)$ be the modular curve over $\mathbf{Q}$ associated to $\Gamma_0(N)$, and let $J = J_0(N)$ denote the Jacobian of $X_0(N)$, which is an abelian variety over $\mathbf{Q}$. Let $\mathbf{T}$ denote the Hecke algebra, which is the subring of endomorphisms of $J_0(N)$ generated by the Hecke operators (usually denoted T_ℓ for $\ell \nmid N$ and U_p for $p|N$). If f is a newform of weight 2 on $\Gamma_0(N)$, then let $I_f = \mathrm{Ann}_{\mathbf{T}} f$ and let A_f denote the associated *newform quotient* $J/I_f J$, which is an abelian variety over $\mathbf{Q}$. If the newform f has integer Fourier coefficients, then A_f is an elliptic curve, and we denote it by E. It is called the *optimal elliptic curve* associated to f and its conductor is N (which we may also call the *level* of E). If A is an abelian variety over a field F, then as usual, Ш(A/F) denotes the Shafarevich-Tate group of A over F.

Theorem 1.1. *Let E be an optimal elliptic curve of prime conductor N. If p is an odd prime such that $E[p]$ is reducible as a* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ *representation*

*This material is based upon work supported by the National Science Foundation under Grant No. 0603668.

over $\mathbf{Z}/p\mathbf{Z}$, then the p-primary component of $Ш(E)$ is trivial. In particular, if an odd prime p divides $|E(\mathbf{Q})_{\mathrm{tor}}|$, then p does not divide $|Ш(E)|$, assuming that $Ш(E)$ is finite.

We shall soon deduce this theorem from a more general result involving abelian subvarieties of $J_0(N)$, which we discuss next. The Eisenstein ideal $\mathfrak{I}$ of $\mathbf{T}$ is the ideal generated by $1 + W_N$ and $1 + \ell - T_\ell$ for all primes $\ell \nmid N$, where W_N denotes the Atkin-Lehner involution. Prop. II.14.2 in [Maz77] implies:

Proposition 1.2 (Mazur)**.** *Let $\mathfrak{m}$ be a maximal ideal of $\mathbf{T}$ with odd residue characteristic. If $J_0(N)[\mathfrak{m}]$ is reducible as a $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ representation over $\mathbf{T}/\mathfrak{m}$, then $\mathfrak{I} \subseteq \mathfrak{m}$.*

Theorem 1.3. *Suppose that N is prime. Let A be an abelian subvariety of $J_0(N)$ that is stable under the action of the Hecke algebra $\mathbf{T}$. If $\mathfrak{m}$ is a maximal ideal of $\mathbf{T}$ containing $\mathfrak{I}$ and having odd residue characteristic p, then $Ш(A)[\mathfrak{m}] = 0$ (equivalently $Ш(A)_{\mathfrak{m}} \otimes_{\mathbf{T}_p} \mathbf{T}_{\mathfrak{m}} = 0$).*

We shall prove this theorem in Section 4. For now, we just remark that our proof follows that of [Maz77, III.3.6] (which proves proves the theorem above for the case where $A = J_0(N)$), with an extra input coming from [Eme03].

Corollary 1.4. *Suppose that N is prime. Let A be an abelian subvariety of $J_0(N)$ that is stable under the action of the Hecke algebra $\mathbf{T}$. If $\mathfrak{m}$ is maximal ideal of $\mathbf{T}$ with odd residue characteristic such that $A[\mathfrak{m}]$ is reducible as a $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ representation over $\mathbf{T}/\mathfrak{m}$, then $Ш(A)[\mathfrak{m}] = 0$ (equivalently $Ш(A)_{\mathfrak{m}} \otimes_{\mathbf{T}_p} \mathbf{T}_{\mathfrak{m}} = 0$).*

Proof. Since $A[\mathfrak{m}]$ is a sub-representation of $J_0(N)[\mathfrak{m}]$, we see that $J_0(N)[\mathfrak{m}]$ is reducible as well. Then by Proposition 1.2, we see that $\mathfrak{I} \subseteq \mathfrak{m}$. The corollary now follows from Theorem 1.3. $\square$

We remark that if A is as in the corollary above, then we do not expect that a statement analogous to the first conclusion of Theorem 1.1 holds if A is not an elliptic curve, i.e., it may not be true that if p is an odd prime such that $A[p]$ is reducible as a $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ representation over $\mathbf{Z}/p\mathbf{Z}$, then $Ш(A)[p] = 0$, although we do not know a counterexample.

Proof of Theorem 1.1. Let f denote the newform corresponding to E and let $\sum_{n>0} a_n(f)q^n$ be its Fourier expansion. For all primes $\ell \nmid N$, T_ℓ acts as multiplication by $a_\ell(f)$ on E, and U_p acts as multiplication by $a_p(f)$ for

all primes $p \mid N$. Also, T_1 acts as the identity. Hence we get a surjection $\phi : \mathbf{T} \to \mathbf{Z}$, whose kernel is I_f. The kernel of the composite $\mathbf{T} \stackrel{\phi}{\to} \mathbf{Z} \to \mathbf{Z}/p\mathbf{Z}$ is then (p, I_f), the ideal of $\mathbf{T}$ generated by p and I_f. Since the composite is also surjective, $\mathbf{T}/(p, I_f) \cong \mathbf{Z}/p\mathbf{Z}$ and so (p, I_f) is a maximal ideal of $\mathbf{T}$, which we denote by $\mathfrak{m}$. Then $\mathfrak{m}$ annihilates $E[p]$, and so $E[p] \subseteq E[\mathfrak{m}]$. Conversely, since $p \in \mathfrak{m}$, $E[\mathfrak{m}] \subseteq E[p]$. Hence $E[\mathfrak{m}] = E[p]$. By hypothesis, $E[p]$ is reducible over $\mathbf{Z}/p\mathbf{Z}$. Hence by the discussion above, $E[\mathfrak{m}]$ is reducible over $\mathbf{T}/\mathfrak{m}$. Then by Corollary 1.4, $Ш(E)[\mathfrak{m}] = 0$. Now $Ш(E)[p]$ is annihilated by p and I_f, hence by $\mathfrak{m}$. Thus $Ш(E)[p] \subseteq Ш(E)[\mathfrak{m}]$, and so $Ш(E)[p] = 0$. If the p-primary part of $Ш(E)$ were non-trivial, then so would $Ш(E)[p]$. Hence the p-primary part of $Ш(E)$ is trivial, as was to be shown. $\square$

In Section 2, we mention the relevance of Theorem 1.1 from the point of view of the second part of the Birch and Swinnerton-Dyer conjecture and the results towards the conjecture coming from the theory of Euler systems. In Section 3, we discuss what one may expect if the level is not prime. Finally, in Section 4, we give the proof of Theorem 1.3.

Acknowledgements: We are grateful to E. Aldrovandi and F. Calegari for answering some questions related to this article, and to W. Stein for helping us use the mathematical software sage. Some of the computations were done on sage.math.washington.edu, which is supported by National Science Foundation Grant No. DMS-0821725.

2 Applications

We first recall the second part of the Birch and Swinnerton-Dyer conjecture (see, e.g.,[Sil92, §16] for details). Let $L_E(s)$ denote the *L-function* of E and let r denote the order of vanishing of $L_E(s)$ at $s = 1$; it is called the *analytic rank* of E. Let $c_p(A)$ denote the order of the arithmetic component group of the special fiber at the prime p of the Néron model of E (so $c_p(E) = 1$ for almost every prime). Let Ω_E denote the volume of $E(\mathbf{R})$ calculated using a generator of the group of invariant differentials on the Néron model of E and let R_E denote the regulator of E.

The *second part of the Birch and Swinnerton-Dyer conjecture* asserts the formula:

$$\frac{\lim_{s \to 1}\{(s-1)^{-r} L_E(s)\}}{\Omega_E R_E} = \frac{|Ш_E| \cdot \prod_p c_p(E)}{|E(\mathbf{Q})_{\mathrm{tor}}|^2} \ . \tag{1}$$

If E is an elliptic curve and N is prime, then by [Eme03, Theorem B], $c_N(E) = |E(\mathbf{Q})_{\mathrm{tor}}|$, so there is some cancellation on the right side of (1). Our result shows that however, in this case, there is no cancellation between the odd parts of $|Ш_E|$ and $|E(\mathbf{Q})_{\mathrm{tor}}|$; in particular, up to a power of 2, the numerator of the right side of (1) is precisely $|Ш_E|$ and the denominator is $|E(\mathbf{Q})_{\mathrm{tor}}|$.

We return to the case where N is arbitrary (not necessarily prime). Suppose E is an elliptic curve whose analytic rank is zero or one. Then by results of [KL89], $Ш_E$ is finite, and moreover, one can use the theory of Euler systems to bound $\mathrm{ord}_p(|Ш_E|)$ for a prime p from above in terms of the order conjectured by formula (1) under certain hypotheses on p. As far as the author is aware, the hypotheses on the prime p include either the hypothesis that the image of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ acting on $E[p]$ is isomorphic to $\mathrm{GL}_2(\mathbf{Z}/p\mathbf{Z})$ or the weaker hypothesis that the $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$-representation $E[p]$ is irreducible. Our result shows that the latter hypothesis is redundant when N is prime, as we now explain in more detail.

Let K be a quadratic imaginary field of discriminant not equal to -3 or -4, and such that all primes dividing N split in K. Choose an ideal $\mathcal{N}$ of the ring of integers $\mathcal{O}_K$ of K such that $\mathcal{O}_K/\mathcal{N} \cong \mathbf{Z}/N\mathbf{Z}$. Then the complex tori $\mathbf{C}/\mathcal{O}_K$ and $\mathbf{C}/\mathcal{N}^{-1}$ define elliptic curves related by a cyclic N-isogeny, and thus give a complex valued point x of $X_0(N)$. This point, called a Heegner point, is defined over the Hilbert class field H of K. Let $P \in J(K)$ be the class of the divisor $\sum_{\sigma \in \mathrm{Gal}(H/K)} ((x) - (\infty))^\sigma$, where H is the Hilbert class field of K.

By [BFH90], we may choose K so that $L(E/K, s)$ vanishes to order one at $s = 1$. Hence, by [GZ86, §V.2:(2.1)], $\pi(P)$ has infinite order, and by work of Kolyvagin, $E(K)$ has rank one and the order of the Shafarevich-Tate group $Ш(E/K)$ of E over K is finite (e.g., see [Kol90, Thm. A] or [Gro91, Thm. 1.3]). In particular, the index $[E(K) : \mathbf{Z}\pi(P)]$ is finite. By [GZ86, §V.2:(2.2)] (or see [Gro91, Conj. 1.2]), the second part of the Birch and Swinnerton-Dyer conjecture becomes:

Conjecture 2.1 (Birch and Swinnerton-Dyer, Gross-Zagier)**.**

$$|E(K)/\mathbf{Z}\pi(P)| = c_E \cdot \prod_{\ell | N} c_\ell(E) \cdot \sqrt{|Ш(E/K)|}, \tag{2}$$

where c_E is the Manin constant of E.

Note that the Manin constant c_E is conjectured to be one, and one knows that if p is a prime such that $p^2 \nmid 2N$, then p does not divide c_E (by [Maz78, Cor. 4.1] and [AU96, Thm. A]).

The following is [Jet08, Cor. 1.5]:

Proposition 2.2 (Jetchev)**.** *Suppose that p is a prime such that $p \nmid 2N$, the image* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ *acting on $E[p]$ is isomorphic to* $\mathrm{GL}_2(\mathbf{Z}/p\mathbf{Z})$ *, and p divides at most one $c_\ell(E)$. Then*

$$\mathrm{ord}_p(|Ш(E/K)|) \leq \mathrm{ord}_p(|Ш(E/K)|_{\mathrm{an}}).$$

We also have:

Proposition 2.3 (Cha)**.** *Suppose that p is an odd prime such that p does not divide the discriminant of K, $p^2 \nmid N$, and the* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$*-representation $E[p]$ is irreducible. Then*

$$\mathrm{ord}_p(|Ш(E/K)|) \leq \mathrm{ord}_p(|Ш(E/K)|_{\mathrm{an}}) + \mathrm{ord}_p\left(\frac{\prod_{\ell | N} c_\ell(E)}{|E(K)_{\mathrm{tor}}|}\right).$$

Proof. This follows from Theorem 21 of [Cha05], in view of the formula in Conjecture 4 of loc. cit. and the fact that under the hypotheses, the Manin constant of E is one by [Maz78, Cor. 4.1]. □

The two results above are typical results coming from the theory of Eulers systems. The inflation-restriction sequence shows that the natural map $Ш(E/\mathbf{Q}) \rightarrow Ш(E/K)$ has kernel a finite group of order a power of 2, hence the above results give bounds on $|Ш(E/\mathbf{Q})|$ as well. Note that the hypotheses of Proposition 2.2 implies that the $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$-representation $E[p]$ is irreducible. Our result shows that if N is prime, then the bound on $|Ш(E/\mathbf{Q})|$ obtained from Proposition 2.2 holds even if the $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$-representation $E[p]$ is reducible and the bound on $|Ш(E/\mathbf{Q})|$ obtained from Proposition 2.3 holds even without the hypothesis that the $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$-representation $E[p]$ is irreducible.

Finally, we remark that Theorem 1.3, which applies not just to elliptic curves, but more generally to abelian subvarieties of $J_0(N)$ that are stable under the action of the Hecke algebra, may have an application to a potential equivariant Tamagawa number conjecture where the quantities in the Birch and Swinnerton-Dyer conjectural formula (analogous to (1) for such abelian varieties) are treated as modules over the Hecke algebra. Also, this more general theorem motivates the need to come up with Euler systems type results for $\mathfrak{m}$-primary parts of the Shafarevich-Tate group for maximal ideals $\mathfrak{m}$ of the Hecke algebra (as opposed to p-primary parts for some prime p).

Table 1:

E	N	r	$p : E[p]$ is reducible	$\lvert E(\mathbf{Q})_{\text{tor}}\rvert$	$\prod_p c_p(E)$	$\lvert Ш_{\text{an}}\rvert$
2366d1	$2 \cdot 7 \cdot 13^2$	0	3	3	3	9
5054c1	$2 \cdot 7 \cdot 19^2$	0	3	1	1	9
46683w1	$3^3 \cdot 7 \cdot 13 \cdot 19$	1	3	3	1	9
10621c1	$13 \cdot 19 \cdot 43$	0	3	3	1	9
33825o1	$3 \cdot 5^2 \cdot 11 \cdot 41$	0	5	1	1	25
40455k1	$3^2 \cdot 5 \cdot 29 \cdot 31$	0	5	1	1	25
52094m1	$2 \cdot 7 \cdot 61^2$	0	5	1	1	25

3 Non-prime conductors

One may wonder what happens if the hypothesis that N is prime is dropped in any of our results above. We searched through Cremona's database [Cre] of elliptic curves of conductor up to 130,000 using the mathematical software sage to find all curves E such that there is an odd prime p such that $E[p]$ is reducible, and p divides the Birch and Swinnerton-Dyer conjectural order of $Ш(E/\mathbf{Q})$. We found several examples, some of which are listed in Table 1. In the table, the first column gives Cremona's label for the elliptic curve, the second column is the prime factorization of the conductor, the third column is the rank of $E(\mathbf{Q})$, the fourth column lists all *odd* primes p such that $E[p]$ is reducible, the fifth column is the order of the odd part of $E(\mathbf{Q})_{\text{tor}}$, the sixth column is the odd part of $\prod_p c_p(E)$, and the last column is the odd part of the Birch and Swinnerton-Dyer conjectural order of $Ш(E/\mathbf{Q})$.

Thus if one believes the second part of the Birch and Swinnerton-Dyer conjecture, then if the hypothesis that N is prime is dropped from the statement of Theorem 1.1 (or of Theorem 1.3 and Corollary 1.4), then the statement is no longer true. Among all the counterexamples that we found (up to level 130,000) the curve 2366d1 has the smallest conductor, all except the curve 46683w1 have analytic rank 0, the curve 10621c1 has the smallest square-free conductor, and the curves 33825o1, 40455k1, and 52094m1 are the only ones for which $p \neq 3$. One might wonder if the weaker statement of Theorem 1.1 that if an odd prime p divides $|E(\mathbf{Q})_{\text{tor}}|$, then p does not divide $|Ш(E/\mathbf{Q})|$ holds if N is not prime. If one assumes the second part of the Birch and Swinnerton-Dyer conjecture, then the curve 10621c1 (among others) shows that this need not hold for $p = 3$ (note also that for this curve,

level is square-free and not divisible by p); however the weaker version does hold in the examples for any prime $p > 3$. The primes 2 and 3 are rather special from the point of view of component groups (e.g., see Remark 2 on p. 175 of [Maz77]). This raises the following question:

Question 3.1. Is it true that if a prime $p > 3$ divides $|E(\mathbf{Q})_{\mathrm{tor}}|$, then p does not divide $|Ш(E/\mathbf{Q})|$, perhaps under the restriction that N is square-free?

While the data mentioned above does support an affirmative answer, in the range of Cremona's database, if p is a prime bigger than 3, then the order of the torsion subgroup is often not divisible by p and the Birch and Swinnerton-Dyer conjectural order of the Shafarevich-Tate group is rarely divisible by p; thus the chance of finding an example where both are divisible by p is very slim. Hence the data is not enough to make the conjecture that the answer to the above question is yes.

4 Proof of Theorem 1.3

As mentioned earlier, our proof follows that of [Maz77, III.3.6] (which proves the theorem above for the case where $A = J_0(N)$), with an extra input coming from [Eme03]. We also take the opportunity to give some details that were skipped in [Maz77, III.3.6].

Let $\mathfrak{m}$ be a maximal ideal of $\mathbf{T}$ containing $\Im$ and having odd residue characteristic p. Following [Maz77, §16], an odd prime number $\ell \neq N$ is said to be *good* if ℓ is not a p-th power modulo N, and $\frac{\ell-1}{2} \not\equiv 0 \bmod p$. As mentioned in [Maz77, p.125], there are always some good primes. Let $\eta = 1 + \ell - T_\ell$ for a good prime ℓ. By [Maz77, II.16.6], $\Im\mathbf{T}_\mathfrak{m}$ is principal and generated by η. We will show below that the map induced on $Ш(A)$ by the map η on A is injective, i.e., $Ш(A)[\eta] = 0$. Then since $\Im\mathbf{T}_\mathfrak{m} \subseteq \mathfrak{m}\mathbf{T}_\mathfrak{m}$, we see that $\eta \in \mathfrak{m}\mathbf{T}_\mathfrak{m}$, and so $Ш(A)[\mathfrak{m}] = Ш(A)_\mathfrak{m}[\mathfrak{m}\mathbf{T}_\mathfrak{m}] = 0$, which proves the theorem.

We now turn to showing that the map induced on $Ш(A)$ by the map η on A is injective. Let $S = \mathrm{Spec}\mathbf{Z}$. Let $\mathcal{J}$ denote the Néron model of $J_0(N)$ over S, and $\mathcal{A}$ the Néron model of A over S. We denote the map induced by η on $\mathcal{J}$ by η_J on $\mathcal{A}$ by η again. Let Δ denote a finite set of primes of $\mathbf{T}$, not containing $\mathfrak{m}$, but containing all other primes in the support of the $\mathbf{T}$-modules $(\ker\eta)(\overline{\mathbf{Q}})$ and $(\mathrm{coker}\,\eta)(\overline{\mathbf{Q}})$. We shall work in the category of $\mathbf{T}$-modules modulo the category of $\mathbf{T}$-modules whose supports lie in Δ. Thus, all equalities, injections, surjections, exact sequences, etc., below shall mean "modulo" Δ. If $\mathcal{G}$ is a group scheme over S, then we shall denote the

associated $fppf$ sheaf on S also by $\mathcal{G}$. All cohomology groups below are for the $fppf$ topology over S.

Now Ш(A) is a submodule of $H^1(S, \mathcal{A})$ by the Appendix of [Maz72]. We will show below that η induces an injection on $H^1(S, \mathcal{A})$. Then the map on Ш(A) induced by η is also injective, as was to be shown. It remains to prove the claim that η induces an injection on $H^1(S, \mathcal{A})$, which is what we do next.

Let C denote the finite flat subgroup scheme of $\mathcal{J}$ generated by the subgroup of $J_0(N)(\mathbf{Q})$ generated by the divisor $(0) - (\infty)$; it is called the cuspidal subgroup in [Maz77, § II.11]. Let Σ denote the the Shimura subgroup of $\mathcal{J}$ as in [Maz77, § II.11]; by [Maz77, II.11.6], it is a μ-type group (i.e., a finite flat group scheme whose Cartier dual is a constant group). Let C_p denote the p-primary component of the cuspidal subgroup C and Σ_p the p-primary component of the Shimura subgroup Σ. As shown in the proof of Lemma 16.10 in Chapter II of [Maz77], η_J is an isogeny. By [Maz77, II.16.6], $\ker \eta_J = C_p \oplus \Sigma_p$ as group schemes, and hence as $fppf$ sheaves. By Theorem 4(i) in [BLR90, §7.5], the map $\mathcal{A} \to \mathcal{J}$ is a closed immersion. Thus $\ker \eta = (\mathcal{A} \cap C_p) \oplus (\mathcal{A} \cap \Sigma_p)$. Let C_A denote the group $H^0(S, \mathcal{A} \cap C_p) = A \cap C_p$. Then, since Σ is a μ-type subgroup, we have

$$H^0(S, \ker \eta) = C_A. \tag{3}$$

Also, since C_p is a constant group scheme and Σ_p is a μ-type group scheme, $C_p \cap \mathcal{A}$ and $\Sigma_p \cap \mathcal{A}$ are admissible group schemes in the sense of § I.1(f) of [Maz77], and so by [Maz77, I.1.7], $H^1(S, C_p \cap \mathcal{A}) = 0$ and $H^1(S, \Sigma_p \cap \mathcal{A}) = 0$ (in the notation of [Maz77, I.1.7]: for $G = C_p \cap \mathcal{A}$, $h^0(G) = \alpha(G)$, and $\delta(G) = 0$ since G is finite, so $h^1(G) = 0$; for $G = \Sigma_p \cap \mathcal{A}$, $h^0(G) = 0$, $\alpha(G) = 0$, and $\delta(G) = 0$ since G is finite by [Maz77, II.11.6], and so $h^1(G) = 0$). Thus

$$H^1(S, \ker \eta) = 0. \tag{4}$$

Consider the short exact sequence:

$$0 \to \ker \eta \to \mathcal{A} \xrightarrow{\eta} \operatorname{im} \eta \to 0. \tag{5}$$

Its associated long exact sequence is:

$$0 \to H^0(S, \ker \eta) \to H^0(S, \mathcal{A}) \xrightarrow{\eta} H^0(S, \operatorname{im} \eta) \to H^1(S, \ker \eta) \to \dots.$$

Now $H^1(S, \ker \eta) = 0$ by (4), so we have an exact sequence:

$$0 \to H^0(S, \ker \eta) \to H^0(S, \mathcal{A}) \xrightarrow{\eta} H^0(S, \operatorname{im} \eta) \to 0. \tag{6}$$

Now consider the short exact sequence:

$$0 \to \mathrm{im}\,\eta \to \mathcal{A} \to \mathrm{coker}\,\eta \to 0.$$

Its associated long exact sequence is:

$$\begin{aligned} 0 \;\to\; & H^0(S, \mathrm{im}\,\eta) \to H^0(S, \mathcal{A}) \xrightarrow{i} H^0(S, \mathrm{coker}\,\eta) \to \\ \to\; & H^1(S, \mathrm{im}\,\eta) \xrightarrow{i'} H^1(S, \mathcal{A}) \to \dots, \end{aligned} \tag{7}$$

where i and i' denote the indicated induced maps. Combining (6) and (7), we get the exact sequence

$$\begin{aligned} 0 \;\to\; & H^0(S, \ker \eta) \to H^0(S, \mathcal{A}) \xrightarrow{\eta} H^0(S, \mathcal{A}) \xrightarrow{i} H^0(S, \mathrm{coker}\,\eta) \to \\ \to\; & H^1(S, \mathrm{im}\,\eta) \xrightarrow{i'} H^1(S, \mathcal{A}) \to \dots. \end{aligned} \tag{8}$$

Claim: The map i is surjective.

Proof. Let $\mathcal{A}^0$ denote the identity component of $\mathcal{A}$ and let Φ denote the quotient (i.e., the component group):

$$0 \to \mathcal{A}^0 \to \mathcal{A} \to \Phi \to 0. \tag{9}$$

By [Eme03, Thm. 4.12(ii) and (iii)], Φ is a constant group scheme and the specialization map $C_A \to \Phi$ is an isomorphism. Hence Φ is killed by η. Also, by the argument in [Gro72, § 2.2] (cf. Prop. C.8 and Cor. C.9 of [Mil86]), η is surjective on $\mathcal{A}^0$ (considered as an $fppf$ sheaf). In view of this, if we apply the map η to the short exact sequence (9) of $fppf$ sheaves and consider the snake lemma, then we see that $\mathrm{coker}\,\eta = \Phi$. Now $H^0(S, \mathcal{A}) = A(\mathbf{Q})$ is a finitely generated abelian group, and by the exactness of (8), the kernel of the map induced by η on this group contains the finite group $H^0(S, \ker \eta) = C_A$. Hence the cokernel of the map induced by η on $H^0(S, \mathcal{A})$ has order at least that of C_A. But by the exactness of (8), this cokernel is isomorphic to the image of i, which is contained in $H^0(S, \mathrm{coker}\,\eta) = H^0(S, \Phi) = C_A$ (from the discussion above), and hence has order at most that of C_A. Thus i must be surjective, as was to be shown. $\square$

Using the claim above, from the exactness of (8), we see that the map i' is injective. Part of long exact sequence associated to (5) is

$$\dots \to H^1(S, \ker \eta) \to H^1(S, \mathcal{A}) \xrightarrow{\eta} H^1(S, \mathrm{im}\,\eta) \to \dots.$$

From this, using the fact that the natural map $i' : H^1(S, \operatorname{im}\eta) \to H^1(S, \mathcal{A})$ in (8) is injective, we get the following exact sequence:

$$H^1(S, \ker\eta) \to H^1(S, \mathcal{A}) \xrightarrow{\eta} H^1(S, \mathcal{A}). \tag{10}$$

But $H^1(S, \ker\eta) = 0$ by (4), and so by (10), η induces an injection on $H^1(S, \mathcal{A})$, as was left to be shown.

References

[AU96] Ahmed Abbes and Emmanuel Ullmo, *À propos de la conjecture de Manin pour les courbes elliptiques modulaires*, Compositio Math. **103** (1996), no. 3, 269–286. MR 97f:11038

[BFH90] D. Bump, S. Friedberg, and J. Hoffstein, *Eisenstein series on the metaplectic group and nonvanishing theorems for automorphic L-functions and their derivatives*, Ann. of Math. (2) **131** (1990), no. 1, 53–127.

[BLR90] S. Bosch, W. Lütkebohmert, and M. Raynaud, *Néron models*, Springer-Verlag, Berlin, 1990. MR 91i:14034

[Cha05] Byungchul Cha, *Vanishing of some cohomology groups and bounds for the Shafarevich-Tate groups of elliptic curves*, J. Number Theory **111** (2005), no. 1, 154–178.

[Cre] J. E. Cremona, *Elliptic curve data*, `http://www.warwick.ac.uk/staff/J.E.Cremona/ftp/data/INDEX.html`.

[Eme03] Matthew Emerton, *Optimal quotients of modular Jacobians*, Math. Ann. **327** (2003), no. 3, 429–458.

[Gro72] A. Grothendieck, *Groupes de monodromie en géométrie algébrique. I*, Springer-Verlag, Berlin, 1972, Séminaire de Géométrie Algébrique du Bois-Marie 1967–1969 (SGA 7 I), Dirigé par A. Grothendieck. Avec la collaboration de M. Raynaud et D. S. Rim, Lecture Notes in Mathematics, Vol. 288.

[Gro91] B. H. Gross, *Kolyvagin's work on modular elliptic curves*, L-functions and arithmetic (Durham, 1989), Cambridge Univ. Press, Cambridge, 1991, pp. 235–256.

[GZ86] B. Gross and D. Zagier, *Heegner points and derivatives of L-series*, Invent. Math. **84** (1986), no. 2, 225–320. MR 87j:11057

[Jet08] Dimitar Jetchev, *Global divisibility of Heegner points and Tamagawa numbers*, Compos. Math. **144** (2008), no. 4, 811–826.

[KL89] V. A. Kolyvagin and D. Y. Logachev, *Finiteness of the Shafarevich-Tate group and the group of rational points for some modular abelian varieties*, Algebra i Analiz **1** (1989), no. 5, 171–196.

[Kol90] V. A. Kolyvagin, *Euler systems*, The Grothendieck Festschrift, Vol. II, Progr. Math., vol. 87, Birkhäuser Boston, Boston, MA, 1990, pp. 435–483.

[Maz72] B. Mazur, *Rational points of abelian varieties with values in towers of number fields*, Invent. Math. **18** (1972), 183–266.

[Maz77] ______, *Modular curves and the Eisenstein ideal*, Inst. Hautes Études Sci. Publ. Math. (1977), no. 47, 33–186 (1978).

[Maz78] ______, *Rational isogenies of prime degree (with an appendix by D. Goldfeld)*, Invent. Math. **44** (1978), no. 2, 129–162.

[Mil86] J. S. Milne, *Arithmetic duality theorems*, Academic Press Inc., Boston, Mass., 1986.

[Sil92] J. H. Silverman, *The arithmetic of elliptic curves*, Springer-Verlag, New York, 1992, Corrected reprint of the 1986 original.